Week 4 Homework Submission File: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
   - Command to inspect permissions:
     ls -l shadow
   - Command to set permissions (if needed):
     sudo chmod 600 /etc/shadow
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
   - Command to inspect permissions:
     ls -l /etc/gshadow
   - Command to set permissions (if needed):
     sudo chmod 600 /etc/gshadow
3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.
   - Command to inspect permissions:
     ls -l /etc/group
   - Command to set permissions (if needed):
     sudo chmod 644 /etc/group
4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.
   - Command to inspect permissions: **ls -l /etc/passwd**
   - Command to set permissions (if needed):

     sudo chmod 644 /etc/passwd

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin`.
   - Command to add each user account (include all five users): sudo adduser *user*
2. Force users to create 16-character passwords incorporating numbers and symbols.
   - Command to edit `pwquality.conf` file:

     vi /etc/security/pwquality.conf
   - Updates to configuration file:

     minlen = 16, dcredit =1, lcredit=1, ocredit=1
3. Force passwords to expire every 90 days.
   - Command to to set each new user's password to expire in 90 days (include all five users):

     sudo chage -M 90 sam

sudo chage -M 90 joe

sudo chage -M 90 amy

sudo chage -M 90 sara

sudo chage -M 90 admin

sudo chage -l can be used to verifies

4. Ensure that only the `admin` has general sudo access.
   - Command to add `admin` to the `sudo` group:

     sudo usermod -aG sudo admin

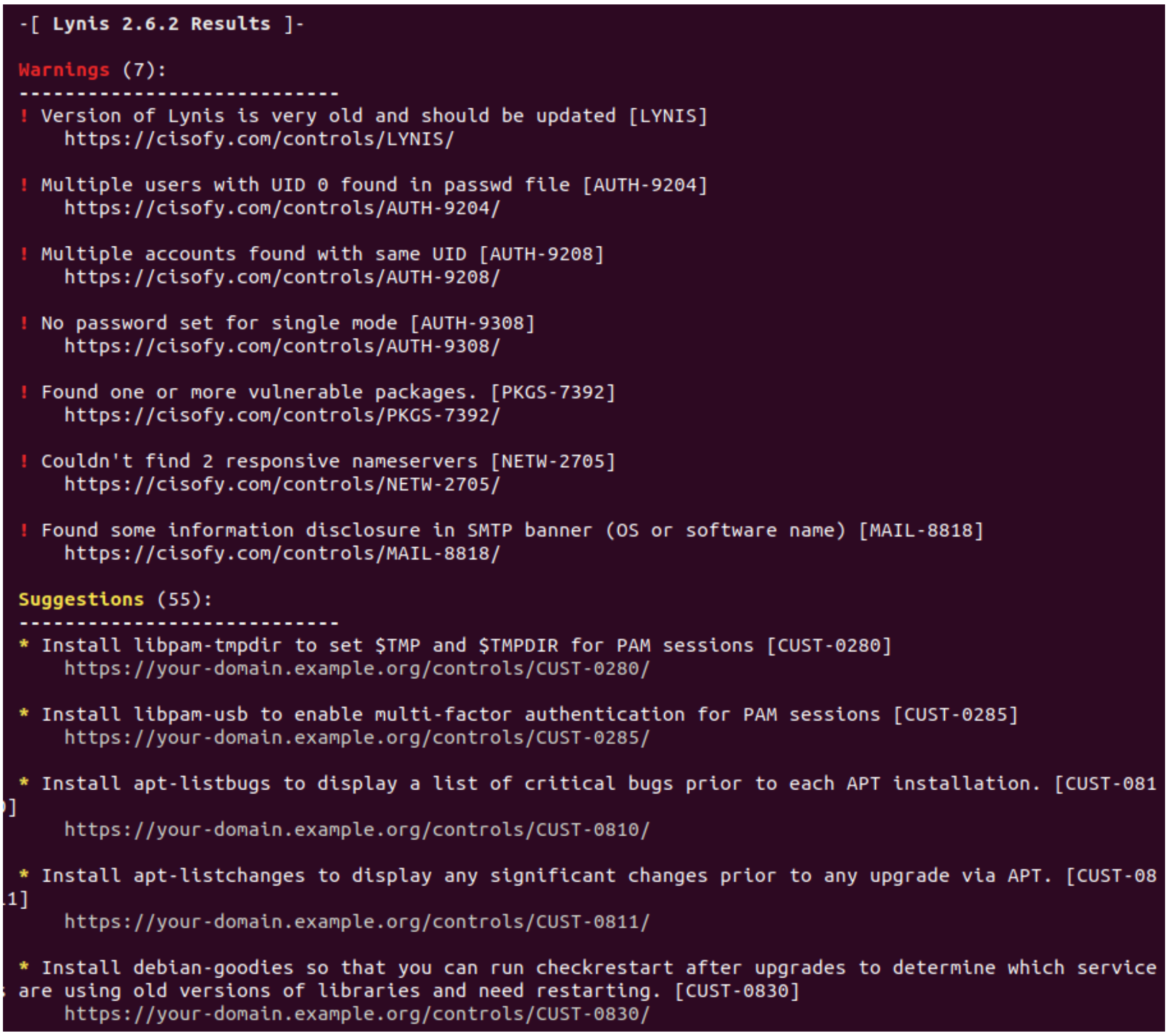
Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.
   - Command to add group:
     sudo addgroup engineer
2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
   - Command to add users to `engineers` group (include all four users):
     sudo usermod -aG general *user*
3. Create a shared folder for this group at `/home/engineers`.
   - Command to create the shared folder:

     sudo mkdir engineers
4. Change ownership on the new engineers' shared folder to the `engineers` group.
   - Command to change ownership of engineer's shared folder to engineer group:
     sudo chown :engineers engineers/

Step 4: Lynis Auditing

1. Command to install Lynis: **sudo apt-get install lynis**
2. Command to see documentation and instructions: **sudo lynis**
3. Command to run an audit: **sudo lynis audit system**
4. Provide a report from the Lynis output on what can be done to harden the system.
   - Screenshot of report output:



```
-[ Lynis 2.6.2 Results ]-

Warnings (7):
----------------------------
! Version of Lynis is very old and should be updated [LYNIS]
    https://cisofy.com/controls/LYNIS/

! Multiple users with UID 0 found in passwd file [AUTH-9204]
    https://cisofy.com/controls/AUTH-9204/

! Multiple accounts found with same UID [AUTH-9208]
    https://cisofy.com/controls/AUTH-9208/

! No password set for single mode [AUTH-9308]
    https://cisofy.com/controls/AUTH-9308/

! Found one or more vulnerable packages. [PKGS-7392]
    https://cisofy.com/controls/PKGS-7392/

! Couldn't find 2 responsive nameservers [NETW-2705]
    https://cisofy.com/controls/NETW-2705/

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
    https://cisofy.com/controls/MAIL-8818/

Suggestions (55):
----------------------------
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
    https://your-domain.example.org/controls/CUST-0280/

* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
    https://your-domain.example.org/controls/CUST-0285/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-081
]
    https://your-domain.example.org/controls/CUST-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-08
1]
    https://your-domain.example.org/controls/CUST-0811/

* Install debian-goodies so that you can run checkrestart after upgrades to determine which service
 are using old versions of libraries and need restarting. [CUST-0830]
    https://your-domain.example.org/controls/CUST-0830/
```

Bonus

1. Command to install chkrootkit:

   sudo apt-get install chkrootkit

2. Command to see documentation and instructions:

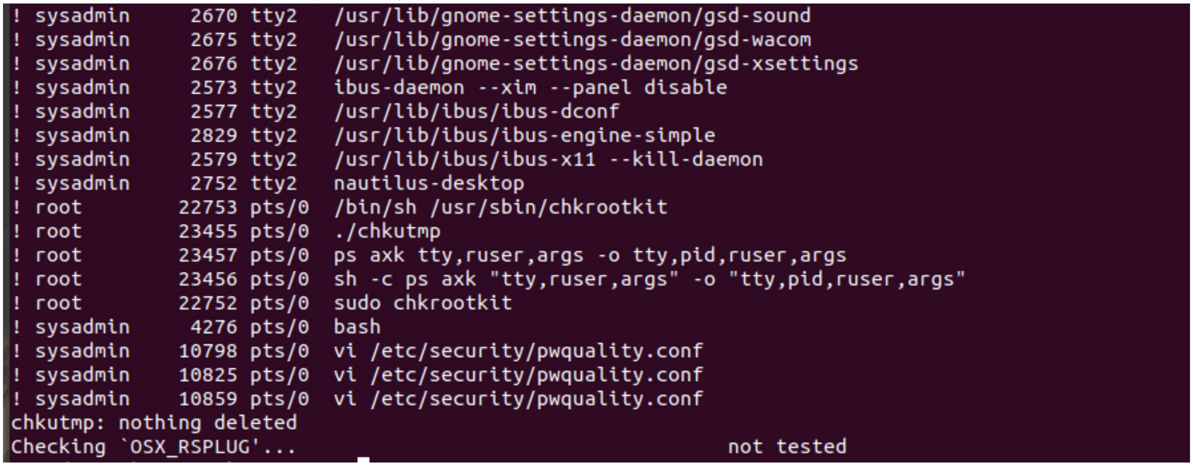
   man chkrootkit

3. Command to run expert mode:

   sudo chkrootkit -x

4. Provide a report from the chrootkit output on what can be done to harden the system.

- Screenshot of end of sample output:



```
! sysadmin     2670 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2675 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2676 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2573 tty2   ibus-daemon --xim --panel disable
! sysadmin     2577 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2829 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2579 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2752 tty2   nautilus-desktop
! root        22753 pts/0  /bin/sh /usr/sbin/chkrootkit
! root        23455 pts/0  ./chkutmp
! root        23457 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        23456 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        22752 pts/0  sudo chkrootkit
! sysadmin     4276 pts/0  bash
! sysadmin    10798 pts/0  vi /etc/security/pwquality.conf
! sysadmin    10825 pts/0  vi /etc/security/pwquality.conf
! sysadmin    10859 pts/0  vi /etc/security/pwquality.conf
chkutmp: nothing deleted
Checking `OSX_RSPLUG'...                                  not tested
```